To All,

The reports about lost/stolen badges are still coming in along with person(s) who are using these stolen items as tools to commit violent crimes. We talked about double checking the identity of these unsolicited and/or unaccompanied person(s) when they ask about information of a USDA site. It would probably be a good idea to extend this word of caution to our employees when they are at home. As you can see by paragraph 1(a) below, the victim thought she did everything correct before opening the door. It may be prudent, if this is an unsolicited encounter, and the employee at home is unaware of any pending visits by law enforcement, that they first call to the police station to verify the questioned visit. This caution should also be extended to delivery personnel and service calls.

A new incident came up during this week's intelligence reports. It brought up the potential dangers of person(s) attempting to compromise natural gas lines. Pre-911, exposed gas lines were not looked upon as a vulnerability to a facility. However, as you can see from paragraph 2, there are people out there that want to exploit this now Post-911 vulnerability. Most gas lines are exposed and easily accessible. We recommend that gas lines be caged to prevent easy access. Each location should coordinate with their local fire department to understand what type of restrictions is present in protecting these gas lines. Because of the gas fumes, it is not advisable to brick in these areas.

Along the same thinking as natural gas lines, is the vulnerability to water supplies. We have been to over 200 USDA sites, and one of the items we look at is well heads. Nine times out of ten, the well head is open and unsecured. So have your sites look at their water source to see if it is properly protected. We will be addressing dams and water reservoirs in the near future and how best to secure these critical infrastructures.

Extortion by hackers is a new and upcoming threat to every aspect of the computer networking environment. As you can read in paragraph 4, the extortionist can be sitting in France and extort a company in Washington DC. To help prevent this crime from occurring, ensure your sites are in compliance with OCIO requirements.

As government employees, we travel quite a bit. And since we are all dedicated servants we bring our laptops with us to work and answer emails. The thieves realize how dedicated we are and now are targeting hotels for unsecured laptops or other valuables. If you have a laptop with you on travel, do not leave it unattended while you are away from the hotel. One recommendation is when you leave the hotel for whatever reason; you take the laptop with you. It's not so much the cost of the laptop, but the information that resides on it. Take a look at paragraph 7 as an example of the potential dangers that could result if vital information is lost/stolen. This paragraph tells of an incident where a government laptop with security assessment information on the hard drive was stolen. The bottom line about this sensitive information is that it could act as a road map on how someone could successfully compromise a surveyed building undetected.

If you are working with this type of sensitive information please refer to DR 3440-2 (SUBJECT: Control and Protection of "Sensitive Security Information) DATE: January 30, 2003

---

1. LAW ENFORCEMENT IMPERSONATORS

a. Man who impersonated federal official ordered jailed until trial

FORT WORTH TX-- When Timothy Nguyen showed up at the residence of a Fort Worth man Sunday to collect a debt; he posed as a federal agent and wore a badge on his belt and a black police ball cap that belonged to a top federal law enforcement official in North Texas.

The lead investigator testified Wednesday at a court hearing that the badge and ball cap had been stolen last summer from the residence of Trinidad Martinez, regional director of the Federal Protective Service, the agency in charge of protecting federal buildings and courthouses.

b. Police impersonator beats Mesa woman - 04:05 PM MST on Thursday, April 8, 2004 - Mesa Arizona

Mesa police are warning residents about a man who is impersonating a police officer and brutally beat a woman.

Xxxxx Xxxxx was assaulted last week when someone she thought was a police officer knocked on her door.

Xxxxx said she looked out of her window before opening the door for the man in the khaki uniform. Upon opening the door, the suspect forced his way in and began punching her.

Xxxxx said when she came to, there was a chair on top of her and her purse was gone. She suffered a dislocated hip and brain swelling.

Xxxxx said she hopes sharing her story will make other people aware of the potential danger.

"If you can't believe it's your own police department, what can you believe? I did everything right before I opened my door for this gentleman," she said.

The suspect is described as a white man in his 30s, about 6 feet 4 inches tall with short, light-brown hair and a clean-cut face.

Anyone with information is asked to call the Mesa Police Department.

2. Gas Line Tampered With At Olean Armory

OLEAN, NY - The FBI and local police are investigating an apparent attempt to blow up the Olean National Guard Armory on Times Square.

Sources familiar with the investigation told The Times Herald that someone tapped a hole in a natural gas line to the building and ran a rubber hose from the hole to a nearby electrical transformer, apparently hoping sparks from the transformer would ignite the natural gas. The sources requested that The Times Herald withhold their names. The tampering was discovered by a New York State Electric and Gas (NYSEG) employee on March 30. The Armory is located on Times Square across from the Olean Police Department. Olean Police Chief Brian Donnelly confirmed that an investigation into tampering with the gas line is ongoing.

3. Was Michigan’s Water Supply Threatened? - April 7, 2004

BURTON, MI - The nation's largest fresh water supply has been threatened by terrorists.

U.S. intelligence learned a little over two weeks ago that Michigan's water supplies could be a target of terrorism. ABC12 has learned that the water pumping station off Center Road is just one of the water supply systems in Mid-Michigan where security was heightened after the potential threat was made. The FBI's Bill Kowalski and Genesee County Drain Commissioner Jeff Wright have confirmed the alert.

4. Hackers Setting Up Racket For 21st Century: Cyber Extortion Threatens Web Sites - April 7, 2004

HARTFORD, CT - The e-mail arrived before dawn with a demand: Pay $30,000 through Western Union for one year of protection.

Otherwise, the note threatened, a crippling computer attack was on its way. It was late January, the Super Bowl was a week away, and betCBSports.com, an online gambling house based in Costa Rica, was being threatened with extortion. Not by neighborhood thugs, but by criminals, probably on the other side of the world, who had hijacked enough computing power to disable the bookmaker's site during the biggest betting event of the year. "The choice is simple," the note explained: "Either you make a deal with us to protect your site from this happening, or you can forget about taking any more bets over the Internet."

5. LARCENIES OCCURRING AT HOTELS - APR 07-04
TO EASTERN SEABOARDS

THIS AGENCY IS INVESTIGATING SEVERAL LARCENIES OCCURRING AT HOTELS ALONG THE NYS THRUWAY. THE SUSPECTS ARE FORCING ENTRY TO THE HOTEL ROOMS AND STEALING LAPTOP COMPUTERS. THE MARRIOTT CHAINS APPEAR TO BE TARGETED FREQUENTLY.

A POSSIBLE SUSPECT VEHICLE IS A GOLD COLORED SUV. PHOTOS OF A W/F SUSPECT ARE AVAILABLE WITH THIS AGENCY

ANY AGENCY INVESTIGATING SIMILIAR INCIDENTS, PLEASE CONTACT SGT ROBERT CONLEY AT 315-435-3081

6. NATIONAL BROADCAST LOST / STOLEN BADGE

LOST OR STOLEN POLICE LIQUOR CONTROL BADGE. SEVEN POINTED YELLOW STAR WITH SILVER METAL POLICE BANNER THAT READS "POLICE - LIQUOR CONTROL - ARIZONA" IN BLUE PRINT. ALSO HAS ARIZONA STATE SEAL AND THE NUMBER 25 ENGRAVED ON THE BOTTOM POINT. LAST SEEN AT FLAGSTAFF PD ON 04062004. IF LOCATED PLEASE CONTACT FLAGSTAFF POLICE DEPARTMENT AT 928 774 1414 ATTENTION DANNY THOMAS. THANK YOU IN ADVANCE FOR YOUR ASSISTANCE.

FLAGSTAFF PD AZ0030100 1151 TCF
15:23:14 04/07/04

7. Phillip Burton Federal Building, 450 Golden Gate Avenue, San Francisco, CA April 6, 2004

A Security Program Manager with the Federal Protective Service reported his laptop was stolen in San Francisco in the vicinity of Bush and Larkin Street. The laptop, a black Dell Latitude ZCPXJ serial number 72CPD01, valued at $600, was taken from the Manager's personal vehicle. Critical information on the laptop was listed as Physical Security Surveys. A Compact Disk was also reported missing (NFI), as well as the leather carrying case and some personal papers. The report of this theft was to be entered into NCIC. The San Francisco PD Case number is 040398536. This is an ongoing investigation.